SYSTEM FOR AUTHENTICATING DIGITAL DATA

ABSTRACT OF THE DISCLOSURE

A system for authenticating digital data capable of preventing change or disguise of data by improvement or interchange in case of no confidentiality in the data itself so as to maintain the data. When writing digital data from an input device to a memory and transferring the digital data from the memory to a receiving device, device authentication is performed between the input device and the memory and between the memory and the receiving device respectively. At the same time, when writing digital data to the memory, in the case of implementing on the digital data an electronic signature by a one-way hash function and also reading from the memory and transferring the digital data, the implemented electronic signature is decrypted so as to transfer the digital data after ensuring that it has not been changed since it was recorded. Thus, it is possible to prevent change or disguise of data by improvement or interchange in case of no confidentiality in the data itself so as to maintain the data.